STATE OF ALABAMA

Information Technology Standard

Standard 660-02S2_Rev B: PDA Security

1. INTRODUCTION:

Personal Digital Assistant (PDA) devices combine mobile computing and networking features in a pocket-sized device. The benefits PDA devices provide: their small size, portability, and their ability to store large amounts of information along with the breadth of communication options available, also expose the organization to many security risks.

2. OBJECTIVE:

Establish implementation requirements for PDA devices connecting to the State of Alabama network.

3. SCOPE:

These requirements apply to PDA devices that are configured to send/receive State of Alabama email or connect to State network applications and/or data and to the system components required to support such devices (including):

- Wireless handheld device (e.g., PDA, Smartphone)
- Software installed on the handheld device by the device manufacturer or wireless carrier (e.g. operating system, internet browser, productivity applications)
- Wireless email product client and server software
- IT Security Policy Management Server
- Gateway Server, located with the IT Security Policy Management Server, providing connection between the wireless handheld device and enterprise network services

Requirements apply to all brands of PDA (including but not limited to Blackberry, Treo, iPhone, and Palm devices).

4. REQUIREMENTS:

4.1 GENERAL REQUIREMENTS

Email redirection (push email) from the Exchange Server to the wireless handheld device shall be State-controlled via a centrally managed server. Desktop or Internet controlled email redirection is not authorized.

Centrally manage the following PDA security controls:

4.1.1 User Authentication

Enforce user authentication using a PIN, password, or passphrase to unlock the device.

The PIN/Password policy shall meet the requirements specified in State IT Standard 620-03S1: Authentication-Passwords.

4.1.2 Inactivity Timeout

The handheld device shall utilize an inactivity timeout whereby the user must reenter their user PIN/password to unlock the device. Set the device inactivity timeout setting to no more than 15 minutes.

4.1.3 Data Wipe

The system administrator shall have the capability to remotely transmit a "data wipe" (hard reset) command to the handheld device. The "Data Wipe" function will erase all data (operating system, applications, and data) stored in user addressable memory on the handheld device.

4.2 DEVICE REQUIREMENTS

4.2.1 User Authentication to Unlock Device

The handheld device must be protected by authenticated logon using a PIN, password, or passphrase. Users shall not bypass device authentication.

4.2.2 Hot-sync Operations

Hot-sync management software shall use some form of access control (e.g., user password is entered before a hot-sync operation can be executed).

Wireless operations shall be disabled when a PDA is connected to the State of Alabama wired network via a hot-sync or other interface cable.

PDA's that transmit receive, store, or process State Sensitive or Confidential information shall not be synced to home or personally-owned PCs.

4.2.3 Physical Safeguards

Asset tag or engrave the device by permanently marking (or engraving) the outer case or an accessible internal area with the agency name, address, and phone number.

Never leave a PDA device in a vehicle where it can be seen through a window. Also keep in mind that the extreme temperature ranges within a vehicle could easily destroy the PDA, and render the information on the device inaccessible.

4.2.4 Device Sanitization

Sanitize PDA devices prior to disposal or reuse; when turning devices in for upgrade, repair or service termination; or upon changes in employment (transfer, resignation, retirement, termination, etc.).

4.2.5 Other Security Controls

Where necessary, restrict or prohibit the use of PDA's with digital cameras (still and video) to protect sensitive and confidential information.

Disable peer-to-peer (ad-hoc) networking capabilities, if so equipped, to prevent inadvertent peer-to-peer communications.

4.3 PERSONALLY-OWNED DEVICE REQUIREMENTS

When communicating with State systems personally-owned PDA's shall comply with the requirements stated in this and other applicable state standards.

Technical support for personally-owned PDA devices is the owner's responsibility. State support personnel will perform only limited support such as provisioning the device so it can receive State email and connect to State network resources and limited diagnostic activities to establish whether a problem is hardware, software, or security incident related.

4.4 LOST DEVICES

User shall immediately report the loss of any PDA (including personally-owned PDA's if used to connect to State networks or store State data) to their manager, IT Manager, or ISO. Administrators shall perform a data wipe command to clear the device memory.

Do not connect a previously lost device to any operational network or system until the device has been properly sanitized (hard reset) and re-provisioned.

4.5 AWARENESS & TRAINING

PDA users shall be provided awareness level training (in accordance with State standards) on the security vulnerabilities presented by use of such devices and on appropriate use.

4.6 PERSONAL USE

Incidental, occasional personal use of state-owned PDA devices is permitted; however, in accordance with The Code of Alabama, Section 36-25-5, state-owned PDA devices shall not be used for "personal gain."

Employees and managers are responsible for exercising good judgment regarding the reasonableness (frequency and duration) of personal use.

Users are permitted to include personal appointments in their state-owned PDA devices to help eliminate scheduling conflicts.

Users may store personal contact information in their state-owned PDA devices.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 660-02: System Security
http://isd.alabama.gov/policy/Policy_660-02_System_Security.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Information Technology Standard 620-03S1: Authentication - Passwords
http://isd.alabama.gov/policy/Standard_620-03S1_Authentication-Passwords.pdf

Information Technology Standard 680-01S4: Media Sanitization
http://isd.alabama.gov/policy/Standard_680-01S4_Media_Sanitization.pdf

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	2/20/2008	
Rev A	7/15/2008	Deleted iPhone exception from Scope.
Rev B	5/11/2009	Deleted forfeiture requirement and text messaging controls; added Personal Use.